PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 :		(11) Numéro de publication internationale:
H04L 9/08	**A1**	**WO 95/20280**
		(43) Date de publication internationale: 27 juillet 1995 (27.07.95)

(21) Numéro de la demande internationale: PCT/FR95/00055

(22) Date de dépôt international: 18 janvier 1995 (18.01.95)

(30) Données relatives à la priorité:
94/00528 19 janvier 1994 (19.01.94) FR

(71) Déposants: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). TELEDIFFUSION DE FRANCE [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75015 Paris (FR).

(72) Inventeur: COUTROT, Françoise; 6, allée de la Croix-Connue, F-35510 Cesson-Sévigné (FR).

(74) Mandataire: BREVATOME; 25, rue de Ponthieu, F-75008 Paris (FR).

(81) Etats désignés: JP, KR, NO, brevet européen (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si de telles modifications sont reçues.

(54) Title: METHOD FOR THE TRANSMISSION AND RECEPTION OF CONDITIONAL ACCESS PROGRAMMES USING CONTROL WORDS SPECIFIC TO SAID PROGRAMMES

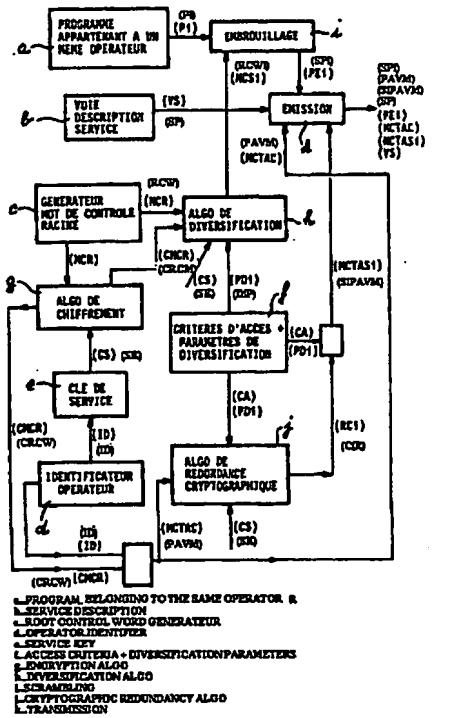
(54) Titre: PROCEDE D'EMISSION ET DE RECEPTION DE PROGRAMMES A ACCES CONDITIONNEL UTILISANT DES MOTS DE CONTROLE SPECIFIQUES AUX PROGRAMMES

(57) Abstract

Method for the transmission and reception of conditional access programmes controlled by the same operator. According to the invention, specific control words (MCSi) are created for various programmes belonging to the same operator based on a root control word corresponding to said operator. The access pass control messages comprise a portion common to all the programmes controlled by the same operator and a portion specific to each programme. The method of the invention is for use in television, radio, data transmission, messaging and the like.

(57) Abrégé

Procédé d'émission et de réception de programmes à accès conditionnel gérés par un même opérateur. Selon l'invention, des mots de contrôle spécifiques (MCSi) sont formés pour divers programmes d'un même opérateur à partir d'un mot de contrôle racine propre à cet opérateur. Les messages de contrôle des titres d'accès comprennent une partie commune à tous les programmes gérés par un même opérateur et une partie spécifique à chaque programme. Application en télévision, radio, transmission de données, messagerie, etc.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Autriche	**GB**	Royaume-Uni	**MR**	Mauritanie
AU	Australie	**GE**	Géorgie	**MW**	Malawi
BB	Barbade	**GN**	Guinée	**NE**	Niger
BE	Belgique	**GR**	Grèce	**NL**	Pays-Bas
BF	Burkina Faso	**HU**	Hongrie	**NO**	Norvège
BG	Bulgarie	**IE**	Irlande	**NZ**	Nouvelle-Zélande
BJ	Bénin	**IT**	Italie	**PL**	Pologne
BR	Brésil	**JP**	Japon	**PT**	Portugal
BY	Bélarus	**KE**	Kenya	**RO**	Roumanie
CA	Canada	**KG**	Kirghizistan	**RU**	Fédération de Russie
CF	République centrafricaine	**KP**	République populaire démocratique de Corée	**SD**	Soudan
CG	Congo			**SE**	Suède
CH	Suisse	**KR**	République de Corée	**SI**	Slovénie
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovaquie
CM	Cameroun	**LI**	Liechtenstein	**SN**	Sénégal
CN	Chine	**LK**	Sri Lanka	**TD**	Tchad
CS	Tchécoslovaquie	**LU**	Luxembourg	**TG**	Togo
CZ	République tchèque	**LV**	Lettonie	**TJ**	Tadjikistan
DE	Allemagne	**MC**	Monaco	**TT**	Trinité-et-Tobago
DK	Danemark	**MD**	République de Moldova	**UA**	Ukraine
ES	Espagne	**MG**	Madagascar	**US**	Etats-Unis d'Amérique
FI	Finlande	**ML**	Mali	**UZ**	Ouzbékistan
FR	France	**MN**	Mongolie	**VN**	Viet Nam
GA	Gabon				

PROCEDE D'EMISSION ET DE RECECPTION DE PROGRAMMES A ACCES CONDITIONNEL UTILISANT MOTS DE CONTROLE SPECIFIQUES AUX PROGRAMMES

Domaine technique

La présente invention a pour objet un procédé d'émission et un procédé de réception de programmes à accès conditionnel, ces programmes étant gérés par un même opérateur.

L'invention s'applique à la télévision, à la radio, à la messagerie, à la transmission de données, etc...

Dans la description qui va suivre, ainsi que dans les revendications, on désignera par "programmes" aussi bien des programmes proprement dits (de télévision, de radio, etc...) que les éléments composant ces programmes, comme par exemple un élément vidéo, ou un élément son, ou un élément de données, etc...

La forte augmentation des supports de diffusion (satellites, câbles, herztien) et des capacités de diffusion sur ces supports (techniques de radio et de télévision numériques) amène les opérateurs de programmes à multiplier les offres de services audiovisuels, sonores ou de données. En particulier, en radio et télévision numériques, grâce aux techniques de compression, les opérateurs de programmes pourront offrir plusieurs programmes pour un coût de transmission équivalent à la transmission d'un seul programme en analogique.

Ainsi, l'offre de services en radio ou en télévision va s'enrichir pour s'organiser en "bouquets"

de programmes, chacun de ces bouquets proposant plusieurs programmes gérés par le même opérateur de programmes. De même, une offre de programmes en multi-diffusion ("Near Video On Demand") peut être proposée : dans ce cas, un même programme de télévision est diffusé simultanément sur plusieurs canaux (logiques) par un même opérateur, avec un décalage dans le temps pour le début de chaque version du programme (le décalage est typiquement de quelques minutes entre chaque début). Ceci permet à l'usager d'accéder à une émission diffusée en multi-diffusion avec un temps d'attente maximum de quelques minutes.

La caractéristique commune de ces nouveaux services, tels que bouquet de programmes ou multi-diffusion, est que plusieurs programmes diffusés simultanément sont gérés par un même opérateur de programmes et seules les conditions d'accès aux programmes eux-mêmes peuvent changer d'un programme à l'autre.

Il est à noter que cette caractéristique s'applique aussi à un programme géré par un opérateur dont les éléments de programme (vidéo, sons, données) sont commercialisés suivant des conditions d'accès différentes. Dans la suite de la description, on appellera "multiprogrammation" l'offre de plusieurs programmes ou éléments de programme par un même opérateur de programmes.

Le principe du contrôle d'accès à de tels services repose sur l'embrouillage du programme (vidéo et/ou sons et/ou données) à l'émission et sur le désembrouillage du message reçu sous le contrôle d'un titre d'accès. Les systèmes d'embrouillage et de désembrouillage sont initialisés par une donnée, qui varie généralement aléatoirement et qui est appelée "mot de contrôle". Les informations décrivant les

critères d'accès au programme ainsi qu'une forme protégée du mot de contrôle sont incluses dans des messages de contrôle des titres d'accès qui accompagnent le programme embrouillé.

Pour accéder à un programme embrouillé, il faut que le dispositif d'accès conditionnel puisse exploiter l'un des messages de contrôle des titres d'accès associés au programme. Dans le cas de programmes appartenant à une multiprogrammation, chacun des programmes ne doit être restitué en clair que par les récepteurs possesseurs des conditions d'accès adéquates pour ce programme.

Etat de la technique antérieure

Les procédés actuels permettant de protéger l'accès à un programme diffusé consistent à affecter à chaque programme un message de contrôle des titres d'accès. Cette technique est largement utilisée dans les services de télévision à péage actuels pour lesquels chaque canal est géré par des opérateurs de programmes différents.

Chaque message de contrôle des titres d'accès comporte en général quatre champs :

- un identificateur (spécifique à un opérateur de programme) du service et de la clé de service utilisée,
- un champ précisant les conditions d'accès à satisfaire pour avoir le droit d'accéder au programme,
- le ou les cryptogramme(s) d'un ou de plusieurs mots de contrôle,

- éventuellement un champ de redondance, qui peut être ajouté afin que le processeur de sécurité ne puisse être utilisé en dehors du contexte prévu.

Quand le processeur de sécurité contient un droit d'accès convenable, c'est-à-dire quand il détient la clé de service indiquée par l'identificateur et l'une des conditions d'accès indiquée par le champ de conditions d'accès, le processeur déchiffre le ou les cryptogramme(s) pour reconstituer le ou les mot(s) de contrôle. Ce mot de contrôle permet au terminal de désembrouiller le programme ou le ou les élément(s) de programme auquel il est associé.

Avec la multiplication des canaux, l'organisation des programmes se fédèrera autour d'offres en multiprogrammation. Avec les techniques actuelles, l'accès conditionnel aux programmes appartenant à un même opérateur de programme nécessitera de produire autant de messages de contrôle des titres d'accès qu'il y aura de conditions d'accès différentes pour accéder à ces programmes.

Ces techniques ne bénéficieront pas de la synergie attendue d'un regroupement de programmes sous la banière d'un même opérateur et, de ce fait, n'optimiseront pas la ressource nécessaire pour diffuser les messages de contrôle d'accès afférant à ces programmes. Ceci est d'autant plus pénalisant que les programmes offerts utilisent une ressource restreinte (cas de la radio utilisant des ressources à partir de 32 kbits/s ou de services de données à large audience tels que presse diffusée, météo, ...).

La présente invention a justement pour but de remédier à ces inconvénients.

Exposé de l'invention

Dans la présente invention, on considère que, comme dans le cas d'une offre de programmes de télévision gérés par des opérateurs de services différents, les utilisateurs de programmes en multiprogrammation acquièrent un ou plusieurs droits d'accès à l'un ou l'autre des programmes offerts par l'opérateur, moyennant les techniques actuelles de gestion des titres d'accès.

L'offre de programmes en multiprogrammation de l'opérateur est ensuite décomposée en autant de programmes qu'il y a de canaux (logiques). Chaque programme (ou chaque élément de programme) est ensuite embrouillé à partir de mots de contrôle spécifiques. Il y a autant de mots de contrôle spécifiques qu'il y a de conditions d'accès différentes pour accéder aux programmes, de façon à garantir la seule réception des programmes aux récepteurs autorisés.

Ces mots de contrôle spécifiques sont calculés par un processeur de sécurité à partir d'un mot de contrôle "racine", valable pour tous les programmes appartenant à un même opérateur de programmes, et diversifiés en utilisant un paramètre de diversification spécifique au programme (référence de canal logique du programme ou de l'élément de programme ou conditions d'accès par exemple).

Aux programmes émis est associée la transmission des messages de contrôle d'accès. Selon l'invention, les messages de contrôle d'accès vont se décomposer en deux parties :

- une première partie, qui est commune à l'ensemble des programmes constitutifs de l'offre de l'opérateur de programmes, contiendra l'identificateur de programme et

le ou les cryptogramme(s) de mots de contrôle "racines" des programmes en multiprogrammation,
- une seconde partie, qui est spécifique de chacun des programmes ou élément de programme constitutifs de l'offre, contiendra les conditions d'accès au programme et la redondance cryptographique qui garantit l'authenticité et l'intégrité du message. Le mot de contrôle spécifique est ensuite recalculé par le processeur de sécurité à partir du mot de contrôle "racine" et du paramètre de diversification retenu, si le processeur de sécurité contient une condition d'accès conforme à l'une de celles qui sont attendues.

Cette technique permet, tout en assurant un accès différencié à des programmes gérés par un même opérateur de programmes, grâce aux différentes conditions d'accès, de réduire considérablement la ressource des données nécessaires pour les messages de contrôle des titres d'accès pour un même opérateur de programmes. Typiquement, dans un mode de fonctionnement avec les techniques actuelles, il est nécessaire de transmettre un débit utile d'environ 1 Kbits/s pour transmettre les messages de contrôle d'accès associés à une condition d'accès (en supposant un taux de répétition de deux messages par seconde). L'utilisation de cette technique permet de "factoriser" des données telles que l'identificateur de service et le mot de contrôle "racine" et de diviser par plus de 2 la taille de la partie spécifique à chaque programme. Ainsi, typiquement, s'il faut une ressource de N Kbits/s pour sécuriser N programmes (ou éléments de programmes) gérés par le même opérateur avec les procédés actuels, cette technique permet de ramener la ressource nécessaire à (N+1)/2 Kbits/s.

Cette technique devient vite efficace en mode "bouquet de programmes" ou multi-diffusion d'un même programme (un même programme peut être en diffusion simultanée sur une dizaine de canaux logiques) auquel cas le gain est d'environ une diminution par 2 de la ressource nécessaire.

Cette technique est par ailleurs d'autant plus appréciable que le service est organisé en programmes ou éléments de programme utilisant une ressource restreinte (par exemple : radio ou services de données à large audience).

De façon plus précise, la présente invention a pour objet un procédé d'émission de programmes à accès conditionnel dans lequel, de façon classique, on embrouille les programmes par un mot de contrôle (MC), on forme un message de contrôle de titres d'accès (MCTA) contenant notamment des critères d'accès (CA) et au moins un cryptogramme d'au moins un mot de contrôle (CMC) obtenu par mise en oeuvre d'un algorithme de chiffrement (AC) et on émet le programme embrouillé (PE) ainsi que le message de contrôle des titres d'accès (MCTA). Le procédé de l'invention est caractérisé par le fait que, pour les programmes (Pi) qui sont gérés par un même opérateur :

a) on forme des mots de contrôle spécifiques (MCSi) propres à chaque programme (Pi) géré par cet opérateur, chaque mot de contrôle spécifique (MCSi) étant obtenu par diversification d'un mot de contrôle unique, dit mot de contrôle racine (MCR) propre à l'opérateur ,la diversification s'opérant à partir, notamment, de paramètres de diversification (PDi) propres à chaque programme géré par cet opérateur,

b) on embrouille chaque programme (Pi) à l'aide du mot de contrôle spécifique (MCSi) qui lui est propre,

c) on constitue les messages de contrôle des titres d'accès (MCTA) en deux parties :

- une première partie, commune à tous les programmes d'un même opérateur et qui est constituée d'un message de contrôle des titres d'accès commun (MCTAC), cette partie commune contenant un identificateur (ID) de l'opérateur de programmes, et de la clé de service (CS) et au moins un cryptogramme (CMCR) du mot de contrôle racine (MCR) propre à chaque opérateur de programme,
- une seconde partie, spécifique à chaque programme (Pi) et qui est constituée d'une part de messages de contrôle des titres d'accès spécifique (MCTASi), propres à chaque programme (Pi) géré par un même opérateur, ces messages spécifiques (MCTASi) contenant les conditions d'accès (CAi) aux divers programmes (Pi) gérés par le même opérateur, les paramètres de diversification (PDi) s'ils sont différents des conditions d'accès (CAi) et une redondance cryptographique (RCi) garantissant l'intégrité du message complet par la première et la seconde partie.

On peut observer, accessoirement, que l'utilisation d'un mot de contrôle racine et la diversification d'un tel mot est déjà révélée par le document FR-A-2 680 589 (EP-A-0 528 730) mais dans un contexte différent qui est celui de l'émission et la réception de programmes personnalisés. La

diversification s'appuie alors sur l'identification de chaque destinataire.

La présente invention a également pour objet un procédé de réception de programmes ayant été émis selon le procédé qui vient d'être défini. De manière générale et connue, dans un tel procédé :

- on reçoit les programmes embrouillés (Pe),
- on sélectionne un programme embrouillé (Pei),
- on vérifie si les critères d'accès (CAi) sont remplis,
- on calcule à partir du message de contrôle des titres d'accès reçu (MCTA), le mot de contrôle (MC) ayant servi à l'embrouillage à l'émission et on désembrouille le programme sélectionné.

Le procédé de l'invention est caractérisé par le fait que, à l'aide de la partie commune du message de contrôle des titres d'accès (MCTAC) propre à l'opérateur, on restitue le mot de contrôle racine (MCR) et, à partir de la partie spécifique du message de contrôle de titre d'accès (MCTASi) propre au programme sélectionné (Pi), on restitue le mot de contrôle spécifique (MCSi) propre à ce programme sélectionné (Pi) en utilisant le mot de contrôle racine (MCR), puis, à l'aide du mot de contrôle spécifique (MCSi) ainsi restitué, on désembrouille le programme sélectionné (Pi).

Brève description des dessins

- la figure 1 illustre un mode de mise en oeuvre du procédé d'émission selon l'invention ;
- la figure 2 illustre un mode de mise en oeuvre du procédé de réception selon l'invention ;

- la figure 3 montre un premier mode d'obtention d'un mot de contrôle spécifique, à partir du mot de contrôle racine dans la phase d'émission ;
- la figure 4 montre un second mode d'obtention d'un mot de contrôle spécifique, à partir du mot de contrôle racine dans la phase d'émission ;
- la figure 5 montre un premier mode d'obtention du mot de contrôle spécifique à partir du cryptogramme du mot de contrôle racine dans la phase de réception, ce mode d'obtention étant associé à la mise en oeuvre, côté émission, du procédé illustré à la figure 3 ;
- la figure 6 montre un second mode d'obtention du mot de contrôle spécifique à partir du cryptogramme du mot de contrôle racine dans la phase de réception, ce mode d'obtention étant associé à la mise en oeuvre, côté émission, du procédé illustré sur la figure 4.

Exposé détaillé de modes de mise en oeuvre

Les programmes gérés par un même opérateur sont notés Pi, où l'indice i prend toutes les valeurs entières allant de 1 à n, si n est le nombre de programmes.

Un programme appartenant à un opérateur comprend des éléments de programmes EP1, ..., EPn souvent appelés composantes du programme (vidéo, audio, données), des données de service permettant de décrire la structure du programme et différentes signalisations nécessaires à l'acquisition du programme. Si le programme est protégé par des moyens d'accès conditionnel, des messages de contrôle d'accès au programme sont transmis sur le même support que le programme dans une voie spécialisée qui regroupe tous

les messages d'accès conditionnel des programmes appartenant à l'opérateur (et éventuellement de tous les autres programmes si l'on veut optimiser le temps de commutation d'un programme à un autre programme).

Les messages de contrôle des titres d'accès des programmes ou éléments de programme appartenant à un même opérateur sont décrits en deux parties selon l'une des caractéristiques de l'invention :

a) une première partie, commune, notée MCTAC et qui contient :
   - l'identificateur de l'opérateur de programme ID et de la clé de service utilisée CS,
   - le ou les cryptogramme(s) d'un ou plusieurs mot(s) de contrôle racine(s) CMCR,

b) une seconde partie, spécifique à chaque programme ou chaque élément de programme ayant une condition d'accès différente et notée MCTASi ; cette seconde partie contient :
   - un champ de conditions d'accès CA,
   - un paramètre de diversification spécifique PDS ; ce paramètre doit être spécifique à l'accès au programme, donc peut être le champ de conditions d'accès ou/et des paramètres tels qu'une référence logique de programme ou d'élément de programme ; ce champ peut ne pas être transmis si le paramètre de diversification choisi se limite au seul champ de conditions d'accès CA, car il est décrit obligatoirement dans la partie spécifique,
   - une redondance cryptographique RC qui garantit l'intégrité du message complet (partie commune + partie spécifique).

La structure de tels messages peut être la suivante :

Partie commune :

Identificateur de service	Cryptogramme(s) de mot(s) de contrôle racine(s)

Parties spécifiques correspondant à n programmes ou éléments de programme appartenant à un même opérateur :

Conditions d'accès 1 + [paramètre de diversification 1]	Redondance cryptographique 1
Conditions d'accès 2 + [paramètre de diversification 2]	Redondance cryptographique 2
.....	.....
Conditions d'accès n + [paramètre de diversification n]	Redondance cryptographique n

La mise en oeuvre de l'invention s'effectue alors schématiquement de la manière suivante.

A) dans la phase d'émission :

- Une voie de description du service VS est produite décrivant l'organisation des programmes, pour chaque programme ou élément de programme et les indicateurs de messages de contrôle des titres d'accès (partie commune et parties spécifiques). Dans la voie de description des services, une indication "multiprogrammation" peut être créée

pour permettre le lien entre programmes appartenant à un même opérateur.

- Les mots de contrôle racine MCR sont tirés aléatoirement et le calcul des mots de contrôle diversifiés MCSi est réalisé pour initialiser chacun des embrouilleurs associés aux éléments de programme.
- Les messages de contrôle d'accès contenant la partie commune et les parties spécifiques sont engendrés et transmis en association avec les programmes.

B) dans la phase de réception :

- On sélectionne, grâce à la voie de description du service, le programme choisi par l'utilisateur ainsi que le(s) message(s) de contrôle d'accès qui permettent de désembrouiller le(s) élément(s) de programme. Ces messages sont constitués de la partie commune et des parties spécifiques à chaque champ de conditions d'accès.
- Le processeur de sécurité du récepteur vérifie, pour chaque message de contrôle d'accès (partie commune et partie spécifique) que le message est intègre, qu'il possède un critère d'accès satisfaisant et il calcule le mot de contrôle diversifié MCSi à partir du mot de contrôle racine MCR et du paramètre de diversification retenu PDi.
- Le mot de contrôle diversifié MCSi initialise le dispositif de désembrouillage qui permet de restituer en clair le programme Pi ou le ou les élément(s) de programme.

Ces diverses opérations sont illustrées sur les figures 1 (en diffusion) et 2 (en réception). Sur ces figures, les différents blocs représentés correspondent

à diverses opérations. On ne doit pas considérer que ces opérations sont effectuées nécessairement par autant de circuits indépendants. L'homme du métier sait que ces opérations sont le plus souvent effectuées globalement, par des microprocesseurs, tant à l'émission qu'à la réception.

Sur la figure 1, les références littérales (a, b, c, ..., i) correspondent aux opérations suivantes :

a) on constitue les programmes à émettre Pi ou les éléments de programme ; tous ces programmes ou éléments de programmes sont gérés par un même opérateur ;

b) on constitue une voie de description de service VS ;

c) on engendre de manière aléatoire un mot de contrôle, valable pour tous les programmes, qui est le mot de contrôle racine MCR ;

d) on définit un identificateur d'opérateur ID ;

e) on définit une clé de service CS associée à l'identificateur ID ;

f) on définit des critères d'accès CA auxquels il faut satisfaire pour avoir le droit d'utiliser la clé de service CS ;

g) à partir du mot de contrôle racine MCR et de la clé de service CS, on met en oeuvre un algorithme, dit de chiffrement AC, pour obtenir un cryptogramme du mot de contrôle racine CMCR ;

h) à partir du mot de contrôle racine MCR et de son cryptogramme CMCR, des paramètres de diversification PDi et de la clé de service CS, on met en oeuvre un algorithme, dit de diversification AD, qui délivre des mots de contrôle spécifiques MCSi ;

i) on embrouille les programmes Pi à l'aide des mots de contrôle spécifiques MCSi et l'on obtient des programmes embrouillés PEi ;

j) à partir de la clé de service CS, de la première partie des messages de contrôle des titres d'accès MCTAC, des critères d'accès CA et des paramètres de diversification PDi, on forme la redondance cryptographique RCi. On constitue alors la seconde partie des messages de contrôle aux titres d'accès MCTASi ;

k) on émet l'ensemble des programmes embrouillés PEi, la voie de description de service VS, la partie commune du message de contrôle d'accès MCTAC, et les parties spécifiques des messages de contrôle des titres d'accès spécifiques MCTASi contenant :
   - les paramètres de diversifiation PDi si ces paramètres ne se limitent pas au seul champ des conditions d'accès CAi ;
   - la redondance cryptographique RCi ;
   - les critères d'accès CAi.

Les opérations effectuées à la réception sont schématisées sur la figure 2 par les blocs 1 à q. Là encore, les opérations sont référencées par des repères littéraux qui correspondent aux paragraphes suivants :

l) on reçoit les programmes ou éléments de programmes embrouillés PEi, la voie de description de service VS, les messages de contrôle des titres d'accès (partie commune MCTAC, et partie spécifique MCTASi contenant les critères d'accès CAi, les paramètres de diversification PDi et la redondance cryptographique RCi) ;

m) on sélectionne un programme ou élément de programme PEi et on extrait les parties communes des messages de contrôle des titres d'accès MCTAC et la partie spécifique du programme choisi MCTASi ;

n) à partir de l'identificateur ID contenu dans MTAC, on restitue la clé de service CS ;

o) à partir des deux parties des messages de contrôle des titres d'accès, MCTAC et MCTASi, on vérifie si les critères d'accès CA sont remplis par les titres d'accès du récepteur et on vérifie la redondance cryptographique RCi, en utilisant la clé de service CS et on délivre le mot de contrôle racine MCR ;

p) à partir du cryptogramme du mot de contrôle racine CMCR, de la clé de service CS, on met en oeuvre un algorithme inverse AC^{-1} de l'algorithme de chiffrement AC qui a été mis en oeuvre à l'émission dans l'opération e) et on met également en oeuvre un algorithme AD de diversification qui est l'algorithme mis en oeuvre à l'émission dans l'opération f), on restitue alors le mot de contrôle spécifique MCSi ;

q) on désembrouille le programme choisi PEi ou les éléments de programme embrouillés à partir du mot de contrôle spécifique MCSi et on obtient, en clair, le programme Pi ou les éléments de programme.

La description qui suit s'applique à tous les programmes de radio, télévision ou de données à péage gérés par un même opérateur de programme et, en particulier, aux systèmes de radio et de télévision

numérique à péage. Cette description s'applique aux services de télévision utilisant le standard MPEG2.

Il est proposé d'ajouter les informations permettant d'introduire des identificateurs de messages de contrôle d'accès communs à tous les programmes de l'opérateur et les identificateurs de messages de contrôle d'accès spécifiques à chacun des programmes.

La table de description d'un service audiovisuel se décompose en quatre niveaux principaux :

N1) **réseau** : ensemble des programmes disponibles sur le réseau, ces programmes étant organisés et regroupés en "multiprogrammations", chaque multiprogrammation étant gérée par un opérateur,

N2) **multiprogrammation** : ensemble des programmes gérés par un même opérateur,

N3) **programme** : entité audiovisuelle ou de données,

N4) **élément de programme** (ou composante) : les composantes constitutives d'un programme (audio, vidéo, data).

Suivant le niveau du caractère commun des programmes, les identificateurs de messages de contrôle des titres d'accès communs et spécifiques se trouveront placés à l'un ou à l'autre des niveaux :

- si le réseau appartient également à un seul opérateur de programme, alors les identificateurs de messages de contrôle d'accès communs seront placés au niveau réseau (N1) et les identificateurs de messages de contrôle d'accès spécifiques au niveau programme (N3) ou éléments de programme (N4) ;
- si le réseau est partitionné en multiprogrammations appartenant à plusieurs opérateurs différents, les identificateurs de messages de contrôle d'accès communs seront

placés au niveau multiprogrammation (N2) et les identificateurs de messages de contrôle d'accès spécifiques au niveau programme (N3) ou éléments de programme (N4) ;

- la technique peut s'avérer déjà intéressante pour optimiser les messages de contrôle des titres d'accès d'un même programme dont les éléments de programme seraient embrouillés suivant des conditions d'accès différentes. Dans ce cas, les identificateurs de messages de contrôle d'accès communs seront placés au niveau programme (N3) et les identificateurs de messages de contrôle d'accès spécifiques au niveau des éléments de programme (N4).

La description de ISO MPEG2 (International Standard Organization-Motion Picture Expert Group 2) dans sa version de novembre 1993 (doc. ISO/IEC 1-13818CD) s'en tenant aux niveaux programme et éléments de programme, le mode de réalisation pourrait être :

- table de description de programme,
  - identificateurs de table,
  - descripteurs de programme,
    - identificateurs du programme,
    - identificateur de messages de contrôle des titres d'accès (partie commune)
    - descripteurs d'élément de programme,
      - identificateur d'élément de programme,
      - identificateur de messages de contôle des titres d'accès (partie spécifique).

Les messages de contrôle des titres d'accès sont conformes à la description donnée ci-dessus, en choisissant comme paramètre de diversification le champ des conditions d'accès :

Partie commune :

Identificateur de service	Cryptogramme(s) de mot(s) de contrôle racine(s)

Parties spécifiques correspondant à n programmes ou éléments de programme appartenant à un même opérateur :

Conditions d'accès 1	Redondance cryptographique 1
Conditions d'accès 2	Redondance cryptographique 2
.....	....
Conditions d'accès n	Redondance cryptographique n

Les modes de mise en oeuvre de l'algorithme de diversification peuvent être divers suivant les techniques cryptographiques utilisées.

En s'inspirant du document déjà cité (FR-A-2 680 589) qui décrit deux variantes de tels algorithmes, on peut retenir, en émission, les deux variantes illustrées sur les figures 3 et 4 et, en réception, les deux variantes correspondantes des figures 5 et 6. Les références littérales utilisées sur ces figures correspondent aux références déjà employées sur les figures 1 et 2.

Dans la variante illustrée sur la figure 3 de la présente demande pour obtenir, dans l'opération h) définie plus haut à propos de la phase d'émission, des mots de contrôle spécifique MCSsi à partir du mot de contrôle racine MCSi, du paramètre de diversification PDi, et de la clé de service CS, on applique l'algorithme de diversification AD au mot de contrôle

racine MCR avec le paramètre de diversification PDi pris comme paramètre de diversification. Pour obtenir le cryptogramme du mot de contrôle racine CMCR, on applique l'algorithme de chiffrement AC au mot de contrôle racine MCR en prenant la clé de service CS comme paramètre de chiffrement (opération g).

Dans la variante de la figure 4, on applique l'algorithme de diversification AD à la clé de service CS en prenant le paramètre de diversification PDi comme paramètre de diversification (opération h1), ce qui donne une clé de service spécifique (CSi) ; puis on applique l'algorithme de déchiffrement AC^{-1} au cryptogramme du mot de contrôle racine CMCR en prenant la clé de service personnalisée comme paramètre de déchiffrement (opération h2), ce qui donne le mot de contrôle spécifique MCSi.

A la réception, dans le cas de la première variante illustrée sur la figure 5, pour obtenir, à partir du cryptogramme du mot de contrôle racine CMCR, de la clé de service CS et du paramètre de diversification PDi, le mot de contrôle spécifique MCSi, on commence par appliquer au cryptogramme du mot de contrôle racine CMCR l'algorithme de déchiffrement inverse AC^{-1} en prenant la clé de service CS comme paramètre de déchiffrement (opération p1), ce qui donne le mot de contrôle racine MCR ; puis on applique à ce mot de contrôle racine MCR l'algorithme de diversification AD en prenant le paramètre de diversification PDi comme paramètre de diversification (opération p2), ce qui donne finalement le mot de contrôle spécifique MCSi.

Dans la seconde variante, illustrée sur la figure 6, pour obtenir, à partir du cryptogramme du mot de contrôle racine CMCR, de la clé de service CS et du

paramètre de diversification PDi, le mot de contrôle spécifique MCSi, on commence (opération p1) par appliquer l'algorithme de diversification AD à la clé de service CS, le paramètre de diversification PDi, ce qui donne une clé de service spécifique CSi ; puis (opération p2) on applique l'algorithme de déchiffrement AC^{-1} au cryptogramme du mot de contrôle racine CMCR en prenant la clé de service spécifique CSi comme paramètre de déchiffrement, ce qui donne finalement le mot de contrôle spécifique MCSi.

Dans quelle que variante que ce soit, ayant obtenu le mot de contrôle spécifique, on l'applique à un générateur pseudo-aléatoire ou à un algorithme d'embrouillage délivrant des suites chiffrantes à l'émission et déchiffrantes à la réception.

Les moyens pour embrouiller et désembrouiller les données peuvent être constitués classiquement par des portes OU-exclusif, dont une entrée reçoit les suites chiffrantes/déchiffrantes et l'autre, les données en clair/embrouillées et dont la sortie délivre les données embrouillées/en clair.

En pratique, les traitements peuvent être réalisés par un processeur de sécurité (carte à mémoire). Le processeur délivre les suites (chiffrantes/déchiffrantes) à appliquer aux données à embrouiller/désembrouiller.

Les exemples de mise en oeuvre des algorithmes de chiffrement et des algorithmes de redondance cryptographique sont connus de l'homme du métier, et ne constituent pas en soi l'objet de l'invention. De tels algorithmes sont illustrés par exemple dans la publication FR-A-2 680 589, à laquelle il a été plusieurs fois fait référence dans la présente description.

REVENDICATIONS

1. Procédé d'émission de programmes à accès conditionnel dans lequel on embrouille les programmes par un mot de contrôle (MC), on forme un message de contrôle de titres d'accès (MCTA) contenant notamment des critères d'accès (CA) et au moins un cryptogramme d'au moins un mot de contrôle (CMC) obtenu par mise en oeuvre d'un algorithme de chiffrement (AC) et on émet le programme embrouillé (PE) ainsi que le message de contrôle des titres d'accès (MCTA),
ce procédé étant caractérisé par le fait que, pour les programmes (Pi) qui sont gérés par un même opérateur :

a) on forme des mots de contrôle spécifiques (MCSi) propres à chaque programme (Pi) géré par cet opérateur, chaque mot de contrôle spécifique (MCSi) étant obtenu par diversification d'un mot de contrôle unique dit mot de contrôle racine (MCR) propre à l'opérateur ,la diversification s'opérant à partir, notamment, de paramètres de diversification (PDi),

b) on embrouille chaque programme (Pi) à l'aide du mot de contrôle spécifique (MCSi) qui lui est propre,

c) on constitue les messages de contrôle des titres d'accès (MCTA) en deux parties :

- une première partie, commune à tous les programmes d'un même opérateur, et qui est constituée d'un message de contrôle des titres d'accès commun (MCTAC), cette partie commune contenant un identificateur de service (ID) de l'opérateur de programmes, et au moins un cryptogramme (CMCR) du mot de contrôle racine (MCR) propre à chaque opérateur de programme,

- une seconde partie, spécifique à chaque programme (Pi) et constituée de messages de contrôle de titre d'accès spécifique (MCTASi), propres à chaque programme (Pi) géré par un même opérateur, ces messages spécifiques (MCTASi) contenant au moins les conditions d'accès (CAi) aux divers programmes (Pi) gérés par le même opérateur, les paramètres de diversification (PDi) s'ils sont différents des conditions d'accès (CAi) et une redondance cryptographique (RCi) garantissant l'intégrité du message complet formé par la première partie commune et la seconde partie spécifique.

2. Procédé selon la revendication 1, caractérisé en ce qu'on émet également un signal de signalisation constitué par une voie de service (VS) qui contient pour chaque programme (Pi) ou élément de programme, des indicateurs de message de contrôle des titres d'accès.

3. Procédé selon la revendication 2, caractérisé en ce que la voie de service contient également une information dite de multiprogrammation permettant de créer un lien entre différents programmes.

4. Procédé selon la revendication 1, caractérisé en ce que, pour obtenir des mots de contrôle spécifiques (MCSi) à partir du mot de contrôle racine (MCR) et de paramètres (PDi) identifiant les programmes et d'une clé de service (CS), on applique au mot de contrôle racine un algorithme de diversification (AD) utilisant la clé de service (CS) et le paramètre de diversification (PDi).

5. Procédé selon la revendication 1, caractérisé par le fait que, pour obtenir des mots de contrôle spécifiques (MCSi) à partir du mot de contrôle racine (MCR), de paramètres (PDi) identifiant les programmes et d'une clé de service (CS), on applique un algorithme de diversification (AD) à la clé de service (CS) en utilisant le paramètre de diversification (PDi), ce qui donne une clé de service spécifique (CSi), puis on applique au cryptogramme du mot de contrôle racine (CMCR) un algorithme de déchiffrement (AC^{-1}) inverse de l'algorithme de chiffrement (AC) en prenant la clé de service spécifique (CSi) comme paramètre de déchiffrement.

6. Procédé de réception de programmes (Pi) émis selon le procédé de la revendication 1, dans lequel

- on reçoit les programmes embrouillés (Pe),
- on sélectionne un programme embrouillé (Pei),
- on vérifie si les critères d'accès (CAi) sont remplis,
- à partir du message de contrôle des titres d'accès reçu (MCTA), on reconstitue le mot de contrôle (MC) ayant servi à l'embrouillage à l'émission et on désembrouille le programme sélectionné,

ce procédé étant caractérisé par le fait que, à l'aide de la partie commune du message de contrôle des titres d'accès (MCTAC) propre à l'opérateur, on restitue le mot de contrôle racine (MCR) et, à partir de la partie spécifique du message de contrôle de titre d'accès (MCTASi) propre au programme sélectionné (Pi), on restitue le mot de contrôle spécifique (MCSi) propre à ce programme sélectionné (Pi) en utilisant le mot de contrôle racine (MCR) puis, à l'aide du mot de contrôle spécifique (MCSi) ainsi restitué, on désembrouille le programme sélectionné.

7. Procédé selon la revendication 6, caractérisé par le fait que, pour obtenir à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et du paramètre de diversification (PDi), le mot de contrôle spécifique (MCSi), on commence par appliquer au cryptogramme du mot de contrôle racine (CMCR) l'algorithme de déchiffrement (AC^{-1}) inverse de l'algorithme de chiffrement (AC) en prenant la clé de service (CS) comme paramètre, ce qui donne le mot de contrôle racine (MCR), puis on applique à ce mot de contrôle racine (MCR) l'algorithme de diversification (AD) en utilisant le paramètre de diversification (PDi)pour obtenir finalement le mot de contrôle personnalisé (MCSi) propre au programme sélectionné.

8. Procédé selon la revendication 6, caractérisé en ce que, pour obtenir, à partir du cryptogramme du mot de contrôle racine (CMCR), de la clé de service (CS) et du paramètre de diversification (PDi), le mot de contrôle spécifique (MCSi), on commence par appliquer l'algorithme de diversification (AD) à la clé de service (CS) en utilisant le paramètre de diversification, pour obtenir la clé de service spécifique (CSi), puis on applique au cryptogramme du mot de contrôle racine (CMCR) l'algorithme de déchiffrement (AC^{-1}) inverse de l'algorithme de chiffrement (AC) en prenant la clé de service spécifique (CSi) comme paramètre de déchiffrement, pour obtenir le mot de contrôle spécifique (MCSi).

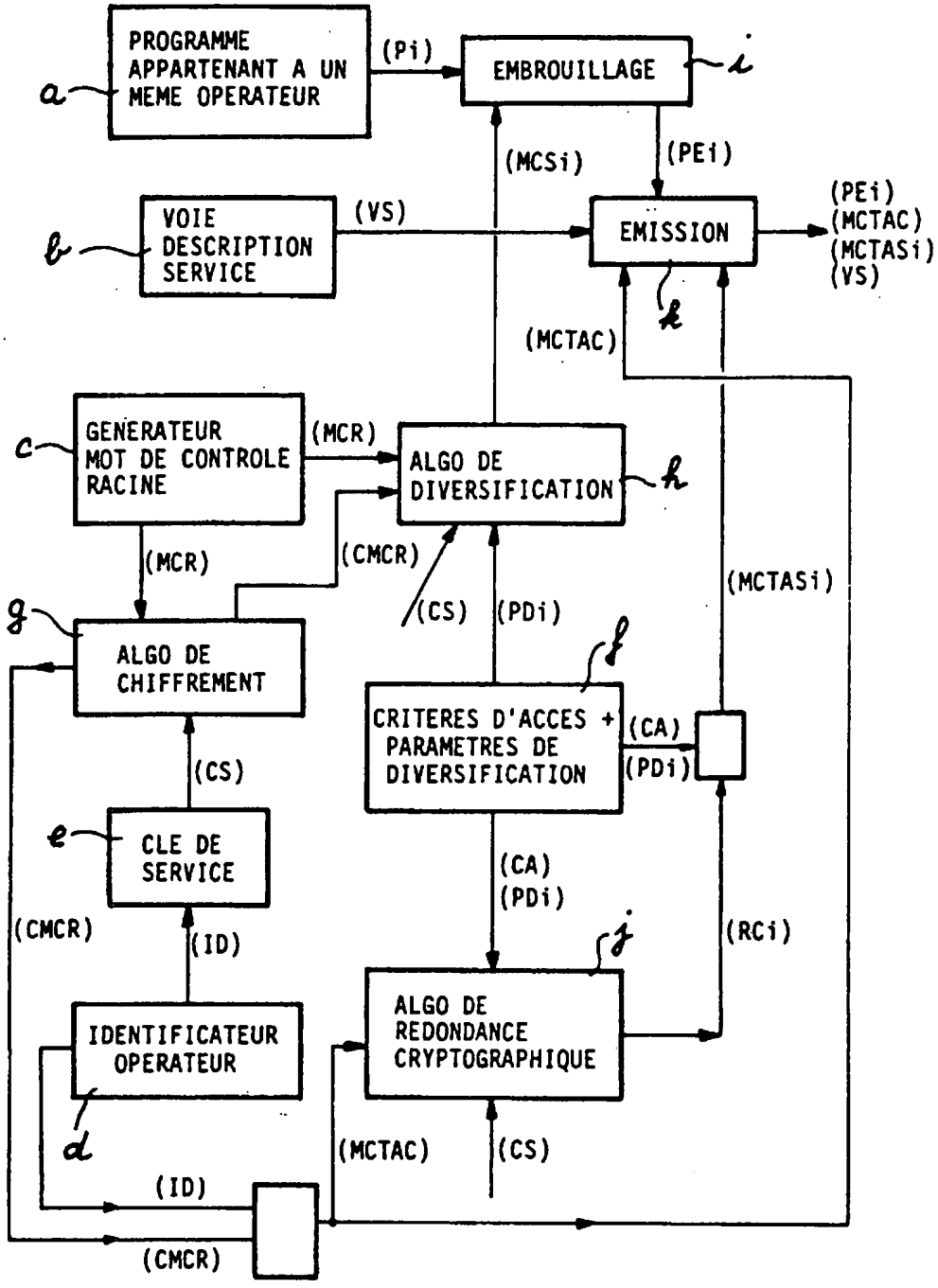

PROGRAMME APPARTENANT A UN MEME OPERATEUR
a
(Pi)
EMBROUILLAGE
i
(MCSi)
(PEi)
VOIE DESCRIPTION SERVICE
b
(VS)
EMISSION
(PEi)
(MCTAC)
(MCTASi)
(VS)
k
(MCTAC)
GENERATEUR MOT DE CONTROLE RACINE
c
(MCR)
ALGO DE DIVERSIFICATION
h
(MCR)
(CMCR)
(CS)
(PDi)
(MCTASi)
g
ALGO DE CHIFFREMENT
f
CRITERES D'ACCES + PARAMETRES DE DIVERSIFICATION
(CA)
(PDi)
(CS)
e
CLE DE SERVICE
(CA)
(PDi)
(CMCR)
(ID)
(RCi)
j
IDENTIFICATEUR OPERATEUR
ALGO DE REDONDANCE CRYPTOGRAPHIQUE
d
(MCTAC)
(CS)
(ID)
(CMCR)

FIG. 1

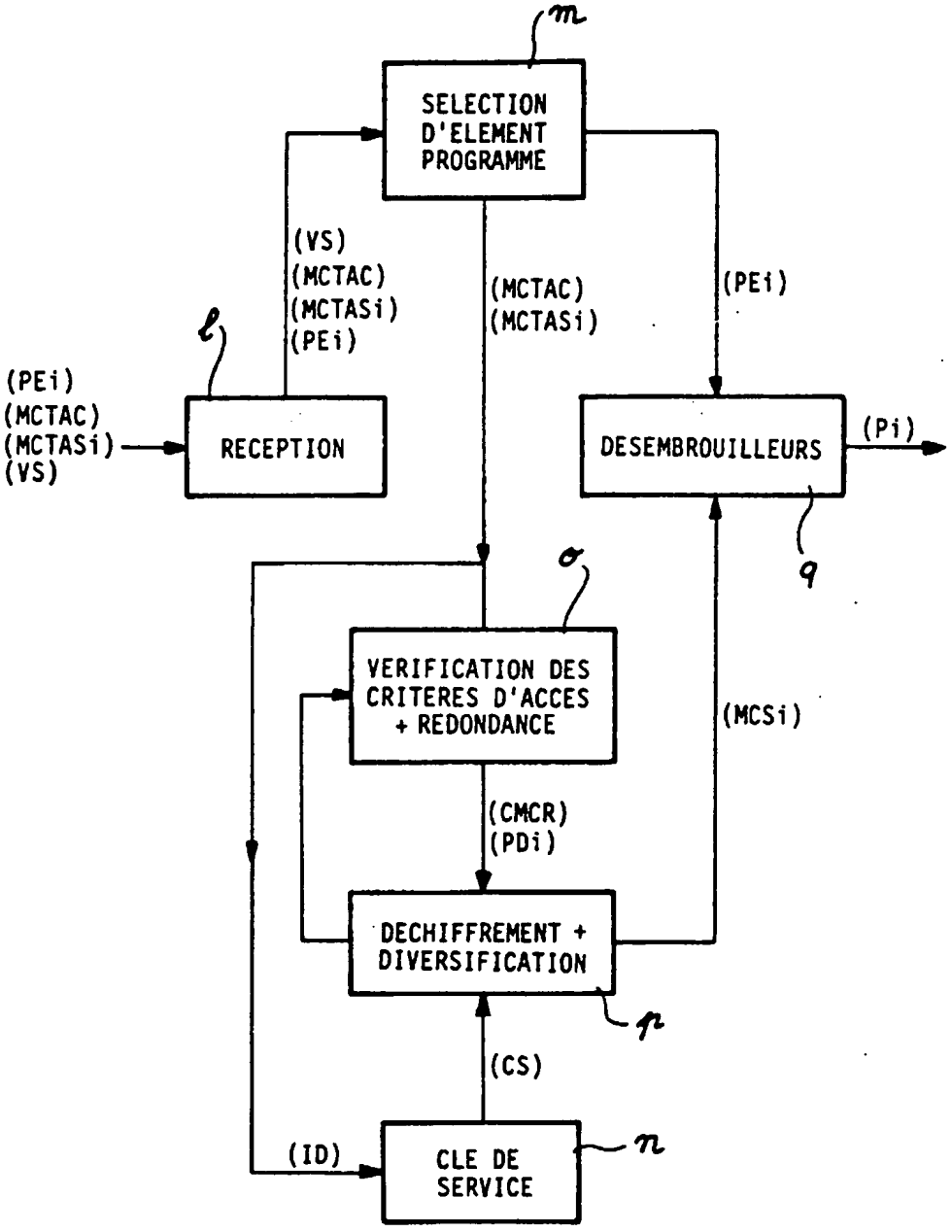

m
SELECTION D'ELEMENT PROGRAMME
(VS)
(MCTAC)
(MCTASi)
(PEi)
(MCTAC)
(MCTASi)
(PEi)
l
(PEi)
(MCTAC)
(MCTASi)
(VS)
RECEPTION
DESEMBROUILLEURS
(Pi)
q
o
VERIFICATION DES CRITERES D'ACCES + REDONDANCE
(MCSi)
(CMCR)
(PDi)
DECHIFFREMENT + DIVERSIFICATION
p
(CS)
(ID)
CLE DE SERVICE
n

FIG. 2

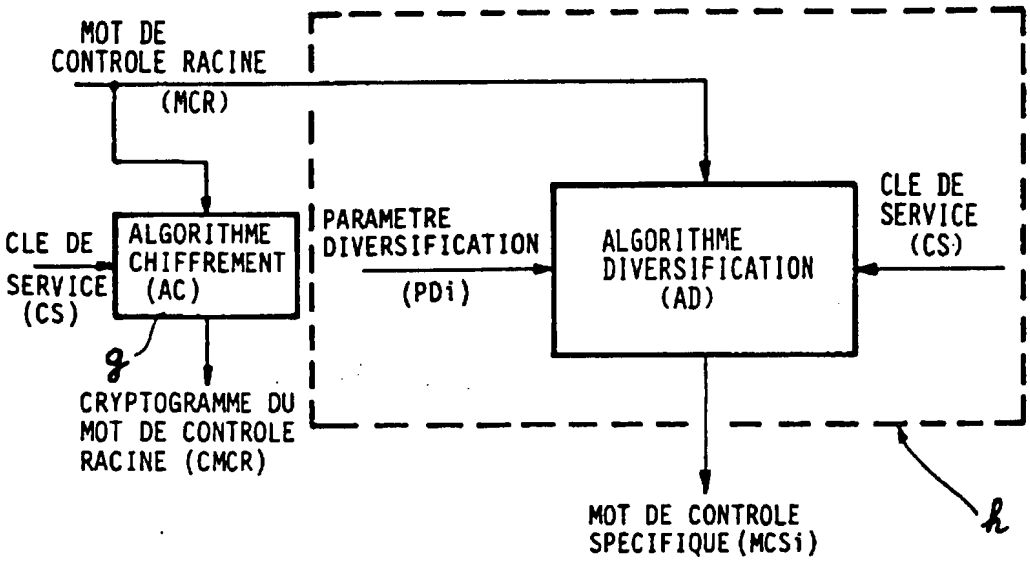

MOT DE CONTROLE RACINE (MCR)
CLE DE SERVICE (CS)
ALGORITHME CHIFFREMENT (AC)
PARAMETRE DIVERSIFICATION (PDi)
ALGORITHME DIVERSIFICATION (AD)
CLE DE SERVICE (CS)
CRYPTOGRAMME DU MOT DE CONTROLE RACINE (CMCR)
MOT DE CONTROLE SPECIFIQUE (MCSi)
g
h

FIG. 3

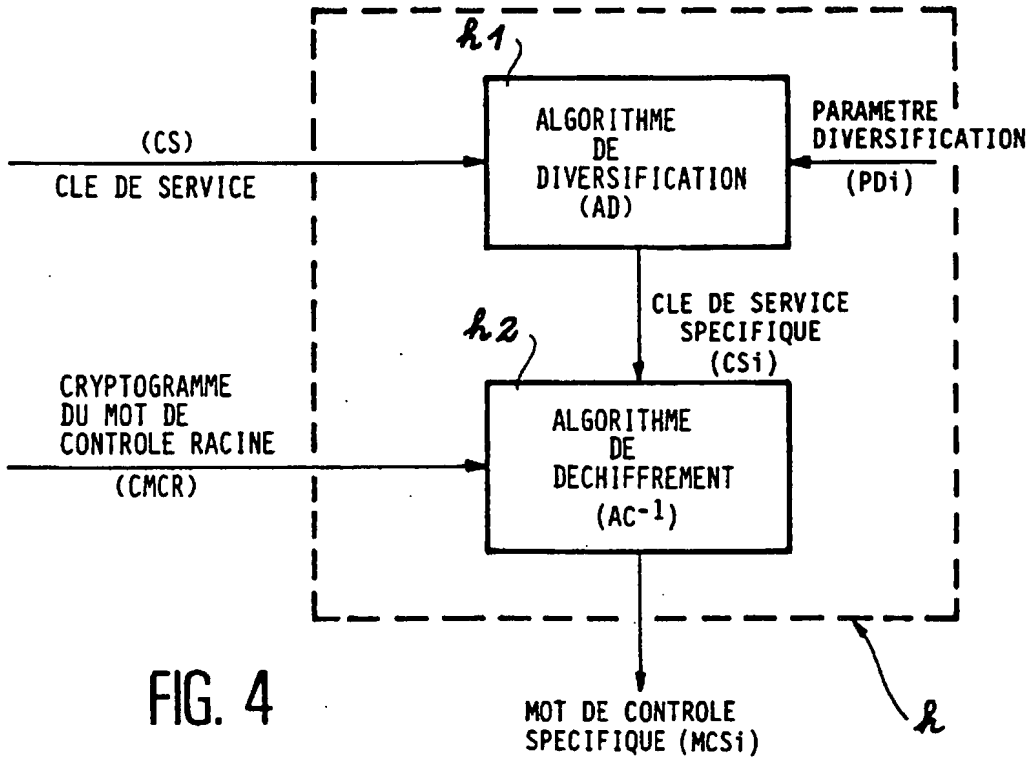

h1
(CS)
CLE DE SERVICE
ALGORITHME DE DIVERSIFICATION (AD)
PARAMETRE DIVERSIFICATION (PDi)
CLE DE SERVICE SPECIFIQUE (CSi)
h2
CRYPTOGRAMME DU MOT DE CONTROLE RACINE (CMCR)
ALGORITHME DE DECHIFFREMENT (AC-1)
MOT DE CONTROLE SPECIFIQUE (MCSi)
h

FIG. 4

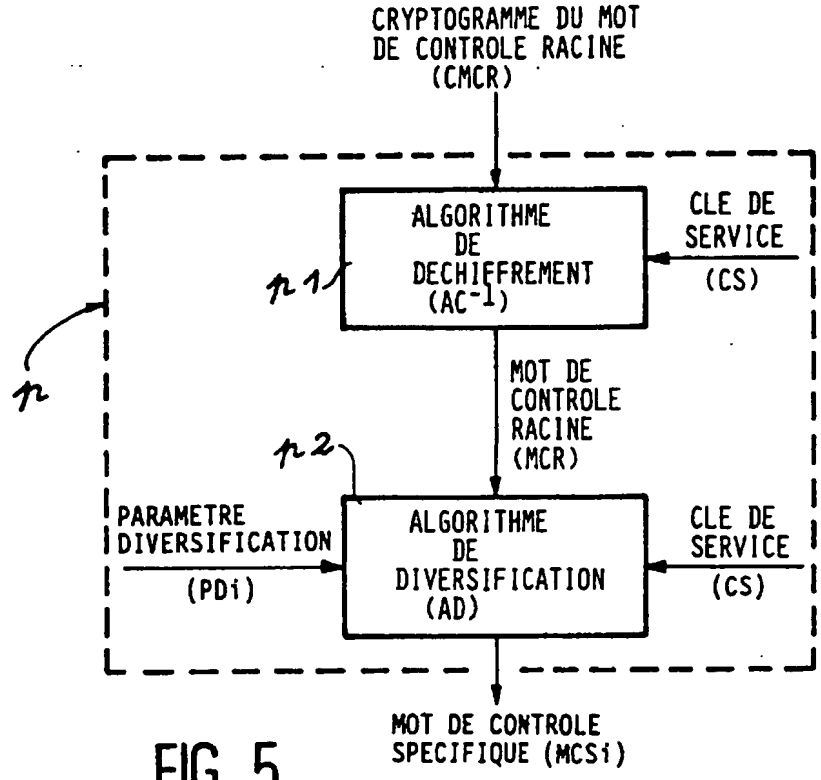

CRYPTOGRAMME DU MOT DE CONTROLE RACINE (CMCR)
ALGORITHME DE DECHIFFREMENT (AC^{-1})
CLE DE SERVICE (CS)
MOT DE CONTROLE RACINE (MCR)
PARAMETRE DIVERSIFICATION (PDi)
ALGORITHME DE DIVERSIFICATION (AD)
CLE DE SERVICE (CS)
MOT DE CONTROLE SPECIFIQUE (MCSi)

FIG. 5

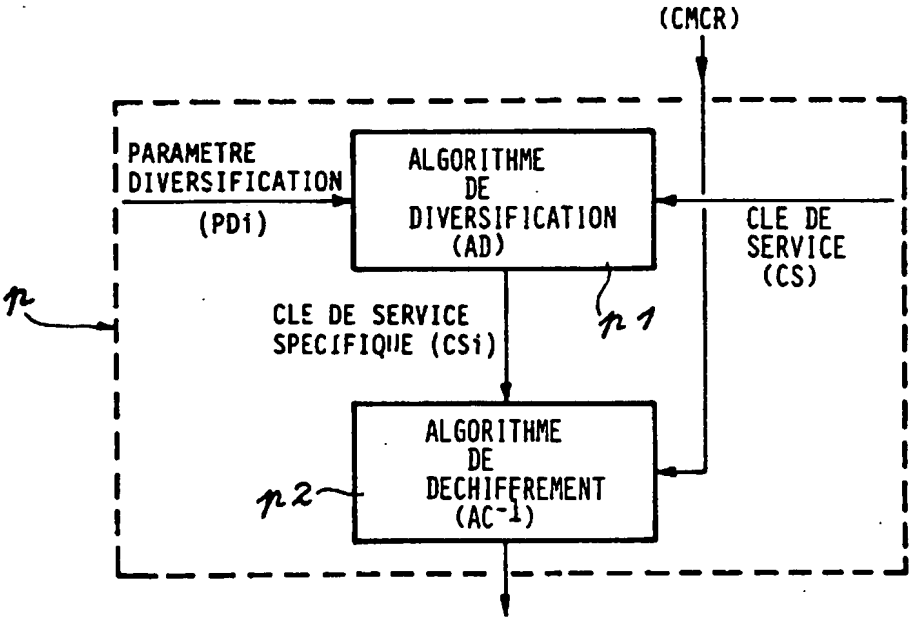

(CMCR)
PARAMETRE DIVERSIFICATION (PDi)
ALGORITHME DE DIVERSIFICATION (AD)
CLE DE SERVICE (CS)
CLE DE SERVICE SPECIFIQUE (CSi)
ALGORITHME DE DECHIFFREMENT (AC^{-1})
MOT DE CONTROLE SPECIFIQUE (MCSi)

FIG. 6

INTERNATIONAL SEARCH REPORT

Interr al Application No
PCT/FR 95/00055

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 528 730 (FRANCE TELECOM) 24 February 1993 cited in the application see abstract see column 1, line 10 - column 3, line 52 see column 4, line 35 - column 5, line 43 see column 5, line 54 - column 7, line 7 see column 7, line 47 - column 8, line 47 see figures 1,3-5,10-13	1,6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 1995	18. 05. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Lydon, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

information on patent family members

Inter ial Application No
PCT/FR 95/00055

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0528730	24-02-93	FR-A-	2680589	26-02-93
		JP-A-	7056831	03-03-95
		US-A-	5301233	05-04-94

RAPPORT DE RECHERCHE INTERNATIONALE

Demi Internationale No
PCT/FR 95/00055

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04L H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP,A,0 528 730 (FRANCE TELECOM) 24 Février 1993 cité dans la demande voir abrégé voir colonne 1, ligne 10 - colonne 3, ligne 52 voir colonne 4, ligne 35 - colonne 5, ligne 43 voir colonne 5, ligne 54 - colonne 7, ligne 7 voir colonne 7, ligne 47 - colonne 8, ligne 47 voir figures 1,3-5,10-13	1,6

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 Mai 1995	18. 05. 95

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Lydon, M

2

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 95/00055

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP-A-0528730	24-02-93	FR-A-	2680589	26-02-93
		JP-A-	7056831	03-03-95
		US-A-	5301233	05-04-94